UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/062,125	01/31/2002	James Kleinsteiber	112-0039US	2526

29855 7590 03/14/2008

WONG, CABELLO, LUTSCH, RUTHERFORD & BRUCCULERI, L.L.P.
20333 SH 249
SUITE 600
HOUSTON, TX 77070

EXAMINER	
HENNING, MATTHEW T	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
03/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/062,125
Filing Date: January 31, 2002
Appellant(s): KLEINSTEIBER ET AL.

Billy C. Allen III
Reg. No. 46,147
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 5/15/2007 appealing from the Office action mailed 10/18/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is incorrect. A correct statement of the status of the claims is as follows:

Claims 1-61 and 72-87 are rejected.

This appeal involves claims 1-61 and 72-87.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows: In addition to claims 1-61 being rejected under 35 USC 112 2nd Paragraph, claims 72, and 76-78 were rejected under the same grounds, and on the same basis.

The appellant's remaining statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,619,657	SUDAMA ET AL.	4-1997
5,422,953	FISCHER	6-1995
5694615	THAPAR ET AL.	12-1997

FIPS PUB 196, "Entity Authentication Using Public Key Cryptography", Feb. 18, 1997, National Institute of Standards and Technology, pp. 1-50

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-61, 72, and 76-78 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The term "secure location", in claims 1, 13, is a relative term which renders the claim indefinite. The term "secure location" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what constitutes “a secure location”. For example, would a fireproof room be considered a secure location. Would a room anchored to the

earth be considered a secure location. Would a plaza with armed guards be considered a secure location. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claim 1 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

The term "less secure location" in claims 1, 13 is a relative term which renders the claim indefinite. The term " less secure location" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what constitutes "a less secure location". For example, would a non-fireproof room be considered a less secure location. Would a room not anchored to the earth be considered a less secure location. Would a plaza with no armed guards be considered a less secure location. Furthermore, the claim gives no basis as to what the location is less secure than. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claim 1 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

The term "substantive" in claims 1, 18, 19, 35, 72, and 76 is a relative term which renders the claim indefinite. The term "substantive" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. In this particular instance, one of ordinary skill in the art would be unable to determine what is considered substantive communication. As such, one of ordinary skill in the art would not be able to determine the scope of the claim. Therefore, claims 1, 18, 19, 35, 72, and 76 are rejected for failing to

particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

Claims 2-34, 36-61, and 77-78 are rejected by virtue of their dependency to an above rejected claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-13, 17-19, 35- 47, 51-53, and 73 are rejected under 35 U.S.C. 102(b) as being anticipated by Sudama et al. (US Patent Number 5,619,657) hereinafter referred to as Sudama.

Regarding claim 1, Sudama disclosed a method of operating a secure network having plurality of network nodes, each node comprising one or more ports (See Sudama Abstract), the method comprising the steps of: locating one or more nodes in a secure location (See Sudama Fig. 2); locating one or more nodes in a less secure location (See Sudama Col. 8 Paragraph 4); communicating selected management information from a primary configuration node to all other nodes in the secure network (See Sudama Col. 5 Paragraph 3), said communicating having the sub-steps of, a first port on a first node sending said management information to a second port on a second node via an communication media exclusively shared by said first port and said second port (See Sudama Col. 8 Paragraph 4, Col. 11 Lines 26-34 and Fig. 2, wherein each end of the physical link must have a physical port connecting the link to the management server); allowing

no management access to said secure network from nodes located in said less secure locations (See Sudama Col. 8 Paragraph 4 and Fig. 2); determining a first list of nodes that may send or receive substantive communication in the secure network (See Sudama Col. 5 Paragraph 3); and prior to substantive communication between any two directly-connected ports, authenticating a link between said directly connected ports (See Sudama Col. 5 Paragraph 3).

Regarding claim 35, Sudama disclosed a specific networking node operating in a secure network, said secure network having a plurality of network nodes, each node comprising one or more ports (See Sudama Fig. 2 and Abstract), said specific networking node comprising: a first port on said specific networking node for receiving selected management information from a primary configuration node (See Sudama Col. 5 Paragraph 3 and Fig. 2), said first port directly communicating with a second port on a second node via an communication media exclusively shared by said first port and said second port (See Sudama Fig. 2 and Col. 8 Paragraph 4); a memory for storing (i) management access information (See Sudama Col. 8 Paragraph 1), and (ii) device connection information specifying nodes or ports that may send or receive substantive communication in the secure network (See Sudama Col. 8 Paragraph 1); and a processor for causing the authentication of the link between said first port and said second port prior to substantive communication between said first and second ports (See Sudama Col. 5 Paragraph 3), wherein said primary configuration node (S1) is configured or adapted to exclusively control a defined set of management functions throughout said secure network (See Sudama Col. 5 Paragraph 3, Col. 7 Lines 31-42, and Col. 8 Paragraph 4).

Regarding claim 73, Sudama disclosed a network comprising: a plurality of devices including one or more switching and routing devices (See Sudama Col. 5 Paragraph 3), any two

of said devices able to inter-communicate only by direct links between each other (See Sudama Fig. 2), all devices able to inter-communicate by forwarding communications through each other (See Sudama Col. 5 Paragraph 3); all of said devices capable of mutually authenticating directly connected links (See Sudama Col. 5 Paragraph 3); one or more pre-designated devices for facilitating management-level control of the network (See Sudama Col. 5 Paragraph 3); and all of said devices carrying a list of all devices allowed on the network (See Sudama Col. 8 Paragraph 1), wherein said primary configuration node (S1) is configured or adapted to exclusively control a defined set of management functions throughout said secure network (See Sudama Col. 5 Paragraph 3, Col. 7 Lines 31-42, and Col. 8 Paragraph 4).

Regarding claims 2-12, and 36-46, Sudama disclosed that said set of management functions comprising the recognition, operation and succession of primary configuration node (See Sudama Col. 5 Lines 20-21); node connection controls for designating nodes to participate in the secure network (See Sudama Col. 4 Lines 28-31), device connection controls that indicate port relationships in said secure network (See Sudama Col. 5 Lines 22-23), and management access controls that restrict management services to a defined set of endpoints (See Sudama Col. 5 Lines 20-23).

Regarding claims 13, and 47, Sudama disclosed that the step of allowing no management access to said secure network from nodes located in said less secure locations comprises the sub-step of distributing a MAC list to every node in said secure network, said MAC list comprising an indication of network endpoints from which management access is acceptable (See Sudama Col. 5 Paragraph 3 and Fig. 2).

Regarding claims 17 and 51, Sudama disclosed that the network endpoints comprise uniquely identified nodes resident in said secure network (See Sudama Fig. 2 and Col. 5 Paragraph 3).

Regarding claims 18 and 52, Sudama disclosed that the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind a port on said primary configuration node to one or more other ports resident in the secure network (See Sudama Col. 5 Paragraph 3 and Col. 8 Paragraph 1 and Fig. 2).

Regarding claims 19 and 53, Sudama disclosed that the step of determining a first list of nodes that may send or receive substantive communication in the secure network comprises the sub-step of distributing a DCC list to every node in said secure network, said DCC list comprising definitions that logically bind each port in said secure network to one or more other ports resident in said network (See Sudama Col. 5 Paragraph 3 and Col. 8 Paragraph 1 and Fig. 2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to

which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 14-16, 20-21, and 48-50, and 54-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama. Sudama disclosed distributing a list of management acceptable nodes in a network (See Sudama Col. 5 Paragraph 3), but failed to disclose that the nodes comprise IP addresses, that IP addresses are associated with SNMP or Telnet or HTTP or API, or that the nodes had ports which were uniquely identified by a world wide name. However, it was well known in the art at the time of invention that network nodes have IP addresses, that IP addresses are associated with access from SNMP or Telnet or HTTP or API, and that network ports were uniquely identified by a world wide name. . Therefore, it would have been obvious to the ordinary skill in the art at the time of invention to employ these well known networking features in the network of Sudama.

Claims 22-31, 33-34, 56-61, and 76-87 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama as applied to claim 1 above, and further in view of FIPS PUB 196 ("Entity Authentication Using Public Key Cryptography") hereinafter referred to as FIPS.

Regarding claims 22 and 56, Sudama disclosed mutual authentication performed between the network devices (See Sudama Col. 5 Paragraph 3) but failed to disclose the use of a three pass authentication scheme in order to do so.

FIPS teaches a method for mutual authentication comprising sending a first fact (R_B) from said first port to said second port (See FIPS Section 3.3 Step 2); at said second node, creating a second-type derivative of said first fact (sS_A), sending said second-type derivative of

said first fact from said second port to said first port (See FIPS Section 3.3 Step 3); at said first node, storing said second-type derivative of said first fact in a first memory; sending a second fact (R_A) from said second port to said first port (See FIPS Section 3.3 Step 3); at said first node, creating a first-type derivative of said second fact (sS_B); sending said first-type derivative of said second fact from said first port to said second port (See FIPS Section 3.3 Step 5); at said second node, storing said first-type derivative of said second fact in a second memory; sending defined information concerning said first node (CertB) from said first port to said second port (See FIPS Section 3.3 Step 5); sending a third-type derivative of said defined information concerning said first node from said first port to said second port (It was well known that certificates included signatures of the hash of the certificate); at said second node, comparing said defined information concerning said first node with said third-type derivative of said defined information concerning said first node (It was also well known to verify the signature of the certificate at the receiver); at said second node, comparing said first type derivative of said second fact with said second fact (See FIPS Section 3.3 Step 6); sending defined information concerning said second node (CertA) from said second port to said first port; sending a third-type derivative of said defined information concerning said second node from said second port to said first port (It was well that certificates included signatures of the hash of the certificate); at said first node, comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node (It was also well known to verify the signature of the certificate at the receiver); and at said first node, comparing said second type derivative of said first fact with said first fact (See FIPS Section 3.3 Step 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of FIPS as the mutual authentication of Sudama. This would have been obvious because the ordinary person skilled in the art would have been motivated to mutually authenticate the nodes prior to communication between the nodes.

Regarding claim 76, Sudama disclosed a routing device for receiving and directing information in a network (See Sudama Fig. 2), comprising: one or more ports for coupling to other routing devices and for authenticating said other routing devices (See Sudama Fig. 2 and Col. 5 Paragraph 3); a memory for storing a list of all said other routing devices that are allowed to substantively communicate on the network (See Sudama Col. 8 Paragraph 1); and a least one logical management access channel that may be disabled through network management control (See Sudama Col. 8 Paragraph 4), but failed to specifically disclose a public and private key pair; or the one or more ports communicating using said public and private key pair.

FIPS teaches a method for mutual authentication comprising sending a first fact (R_B) from said first port to said second port (See FIPS Section 3.3 Step 2); at said second node, creating a second-type derivative of said first fact (sS_A), sending said second-type derivative of said first fact from said second port to said first port (See FIPS Section 3.3 Step 3); at said first node, storing said second-type derivative of said first fact in a first memory; sending a second fact (R_A) from said second port to said first port (See FIPS Section 3.3 Step 3); at said first node, creating a first-type derivative of said second fact (sS_B); sending said first-type derivative of said second fact from said first port to said second port (See FIPS Section 3.3 Step 5); at said second node, storing said first-type derivative of said second fact in a second memory; sending defined information concerning said first node (CertB) from said first port to said second port (See FIPS

Section 3.3 Step 5); sending a third-type derivative of said defined information concerning said first node from said first port to said second port (It was well known that certificates included signatures of the hash of the certificate); at said second node, comparing said defined information concerning said first node with said third-type derivative of said defined information concerning said first node (It was also well known to verify the signature of the certificate at the receiver); at said second node, comparing said first type derivative of said second fact with said second fact (See FIPS Section 3.3 Step 6); sending defined information concerning said second node (CertA) from said second port to said first port; sending a third-type derivative of said defined information concerning said second node from said second port to said first port (It was well that certificates included signatures of the hash of the certificate); at said first node, comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node (It was also well known to verify the signature of the certificate at the receiver); and at said first node, comparing said second type derivative of said first fact with said first fact (See FIPS Section 3.3 Step 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of FIPS as the mutual authentication of Sudama. This would have been obvious because the ordinary person skilled in the art would have been motivated to mutually authenticate the nodes prior to communication between the nodes.

Regarding claim 79, Sudama disclosed a network configuration entity configured or adapted to exclusively control a defined set of management functions throughout a secure network, said secure network comprising a plurality of switching devices, said set of

management functions comprising (i) the recognition, operation and succession of the network configuration entity and (ii) switch connection controls for designating devices to participate in the secure network (See Sudama Col. 5 Paragraph 3), said network configuration entity comprising; a memory for storing an NCE list, said NCE list comprising an indication of each device in the network that may operate as said network configuration entity (See Sudama Col. 5 Paragraph 3); an SCC list, said SCC list comprising an indication of each device allowed to participate in said secure network (See Sudama Col. 5 Paragraph 3); but failed to specifically disclose a first secret fact; a first port for sending said secret fact to a second switch; a second port for receiving, a second-type derivative of said first secret fact from said second switch, pre-defined information about said second switch, and a third-type derivative of said pre-defined information about said second switch; and a processor for (i) causing a comparison between said first secret fact and said second-type derivative of said first secret fact, and (ii) causing a comparison between said pre-defined information about said second switch and said third-type derivative of said pre-defined information about said second switch.

FIPS teaches a method for mutual authentication comprising sending a first fact (R_B) from said first port to said second port (See FIPS Section 3.3 Step 2); at said second node, creating a second-type derivative of said first fact (sS_A), sending said second-type derivative of said first fact from said second port to said first port (See FIPS Section 3.3 Step 3); at said first node, storing said second-type derivative of said first fact in a first memory; sending a second fact (R_A) from said second port to said first port (See FIPS Section 3.3 Step 3); at said first node, creating a first-type derivative of said second fact (sS_B); sending said first-type derivative of said second fact from said first port to said second port (See FIPS Section 3.3 Step 5); at said second

node, storing said first-type derivative of said second fact in a second memory; sending defined information concerning said first node (CertB) from said first port to said second port (See FIPS Section 3.3 Step 5); sending a third-type derivative of said defined information concerning said first node from said first port to said second port (It was well known that certificates included signatures of the hash of the certificate); at said second node, comparing said defined information concerning said first node with said third-type derivative of said defined information concerning said first node (It was also well known to verify the signature of the certificate at the receiver); at said second node, comparing said first type derivative of said second fact with said second fact (See FIPS Section 3.3 Step 6); sending defined information concerning said second node (CertA) from said second port to said first port; sending a third-type derivative of said defined information concerning said second node from said second port to said first port (It was well that certificates included signatures of the hash of the certificate); at said first node, comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node (It was also well known to verify the signature of the certificate at the receiver); and at said first node, comparing said second type derivative of said first fact with said first fact (See FIPS Section 3.3 Step 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of FIPS as the mutual authentication of Sudama. This would have been obvious because the ordinary person skilled in the art would have been motivated to mutually authenticate the nodes prior to communication between the nodes.

Regarding claims 23, 33, 58, and 81, the combination of Sudama and FIPS disclosed that the step of comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node, comprises the sub-steps of: reversing the derivation of the third-type derivative of said defined information concerning said second node; and comparing the result of said reversal with said defined information concerning said second node (It was well known at the time of invention that a signature was decrypted using the public key of the certificate authority and compared with the signed data to verify the signature).

Regarding claims 24, 59, and 82, the combination of Sudama and FIPS disclosed that the step of comparing said defined information concerning said second node with said third-type derivative of said defined information concerning said second node, comprises the sub-steps of: making a third-type derivative of said defined information concerning said second node; and comparing the made third-type derivative with the received third-type derivative (It was well known at the time of invention that a signed hash was decrypted using the public key of the certificate authority and compared with the hash of the certificate to verify the signature).

Regarding claim 25-27, the combination of Sudama and FIPS disclosed that the step, at said second node, of creating a second-type derivative of said first fact comprises the sub-steps of: encoding said first fact to yield an encoded first fact; and encrypting said encoded first fact (It was well known at the time of invention that a signature was created by hashing the data to be signed and then encrypting the hash with a private key of a public key pair).

Regarding claims 28-29, and 85, the combination of Sudama and FIPS disclosed that defined information concerning said first node comprises encryption key information and that

encryption key information comprises a public key uniquely associated with said first node (See FIPS Section 3.1.4).

Regarding claims 30-31, 34, 61, and 84, the combination of Sudama and FIPS disclosed that the third-type derivative is created using a private key uniquely associated with an encryption key authority, said encryption key authority associated with said first node and said second node (See FIPS Section 3.1.4).

Regarding claims 57, and 80, Sudama and FIPS disclosed that the third port and the fourth port are the same port (See Sudama Fig. 2).

Regarding claim 60, Sudama and FIPS disclosed that the second-type derivative is associated with the third node (See FIPS Section 3.3 Step 3).

Regarding claim 77, Sudama and FIPS disclosed that the certificate authority for the public and private key pair is not the entity controlling management access to said routing device (See FIPS Section 3.1.4).

Regarding claim 78, Sudama and FIPS disclosed a memory for storing distributed time service information (It was well known in the art for network devices to contain network time service information).

Regarding claim 83, Sudama and FIPS disclosed that the second-type derivative is associated with said second switch (See FIPS Section 3.3).

Regarding claims 86-87, Sudama and FIPS disclosed that the first secret fact is a random nonce (See FIPS Section 3.3).

Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama and FIPS as applied to claim 30 above, and further in view of Fischer (US Patent Number 5,422,953).

Sudama and FIPS disclosed the use of certificates (See the rejection of claim 22 above), but failed to disclose the certificate being issued by the manufacturer of the node devices.

Fischer teaches that a manufacturer of a device can also be the issuer of the devices public key certificate (See Fischer Col. 6 Paragraph 3).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Fischer in the network system of Sudama and FIPS by having the manufacturer of the network devices issue the certificates to the devices. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide assurance through the certificate that network device was secure.

Claims 72 and 74 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama as applied to claim 73 above, and further in view of Thapar et al. (US Patent Number 5,694,615) hereinafter referred to as Thapar.

Sudama disclosed a method of securing a fabric, said fabric having a plurality of switches all communicatively coupled together, said method comprising the steps of: only allowing communication between pre-defined pairs of said devices as specified by a network operator (See Sudama Col. 5 Paragraph 3); and only allowing substantive communication between devices that are on a pre-defined list of allowed devices (See Sudama Col. 5 Paragraph 3), said pre-defined list stored on a memory in each of said plurality of devices (See Sudama Col. 8 Paragraph 1); and only allowing substantive communication between directly connected ports that have been mutually authenticated (See Sudama Col. 5 Paragraph 3), but failed to disclose the system being used in a fibre channel.

Thapar teaches that the fibre channel addresses the need for very fast data transfers (See Thapar Col. 1 Lines 18-26).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Thapar in the communication network of Sudama by replacing the routers of Thapar with Fibre Channel routers. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow for very fast transfers of large volumes of data.

Claim 75 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sudama as applied to claim 73 above, and further in view of applicant admitted prior art.

Sudama disclosed a network of routers (See Sudama Fig. 2), but failed to disclose the routers being in locked rooms.

Applicants admitted on page 2 paragraph 2 of the specification that the prior art secured computer equipment by locking it in a room.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of the applicants' admitted prior art in the networking system of Sudama by locking the management devices in rooms. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect the devices against tampering and theft.

(10) Response to Argument

Issue #1

In response to the Appellant's argument, with regards to the rejection of the claims under 35 USC 112 2nd Paragraph, that one ordinary skill in the art would understand the entire scope of "a secure network", "a less secure network", "substantive communication", the examiner disagrees. The Appellant has argued that in light of the specification the scope of these terms is clear, however, the examiner points out that these terms are relative terms, and as such the specification is required to provide a standard for ascertaining the requisite degree. However, the requisite degree has not been specifically established in the specification, but rather only a few examples have been provided. Furthermore, some of these examples include further relative terminology. For instance, in page 13 of the Appeal Brief, in an attempt to show definiteness of "a secure location" and "a less secure location" the Appellant has cited the following:

> "That is the ability to locate network equipment in buildings, rooms or cabinets with ***varying degrees of physical security*** as long as the network configuration entity is located in an area of ***sufficient*** physical security".

This only raises the question of "what falls within the scope of sufficient physical security?". Further, the Appellant has cited the following:

> "The latter case provides enhanced ***security*** … by use of ***a secure locked room***."

This attempt to provide the requisite degree of the relative term "secure location" uses the relative term "secure". This provides no definiteness to the claim language. Further still, the Appellant's argument on page 14 of the appeal brief, that "the level of security at the secure location be sufficient to address some threat to network security that was not addressed by the less-secure location" sets the requisite degree, the examiner points out that this can be found

nowhere in the specification. Furthermore, the claims don't recite "a first location" and "a second location which is less secure than the first location".

Regarding the relative term "**substantive** communication", the Appellant's argue that one of ordinary skill in the art would clearly understand this to distinguish from system overhead. The examiner disagrees. The word "substantive" suggests that the communication is meaningful, and once again, the specification fails to provide a requisite degree such that one of ordinary skill in the art could ascertain the scope of "substantive communication". For instance, in the same network, one person of ordinary skill in the art may consider one message, an email for example, to be substantive, while another person of ordinary skill in the art may not.

Because the specification does not provide a means for determining the requisite degree of each of these claim terms, the examiner believes that the rejection is proper and therefore should be maintained.

Issue #2

Regarding the Appellant's argument, regarding the rejection of claim 1 under 35 USC 102(b), that Sudama does not teach or suggest "locating one or more nodes in a secure location" or "locating one or more nodes in a less secure location", the examiner disagrees. First, the examiner notes that the claims do not require "a **physically** secure location" and "a less **physically** secure location", and as such the examiner has not read this into the claim language. Fig. 2 of Sudama shows four "nodes", S1-S4. Col. 8 Paragraph 4 of Sudama recites:

> FIG. 2 shows an illustrative network configuration of four (4) networked systems, S1-S4 for employing the security facility of the present invention. Each system S contains a single management server M and one or more hosts C. More particularly, the network in FIG. 2 consists of a number of host systems C1

> through C6 with management servers M1 through M4 arranged in a hierarchical topology. **Management operations can follow a trusted path downstream from M1 to M4, however, no trusted path exists for routing management operations upstream. For instance, M2-M4 cannot transmit a management operation to M1. Also, in this hierarchical topology, M4 cannot forward a request to any other management server M.** The management server M1 administers management services for a host system C1 as well as transmissions to a second management server M2. The management server M2 administers management services for the hosts C2 and C3 as well as transmissions to a third management server M3. The management server M3 administers management services for a host system C4 as well as transmissions to a fourth management server M4, which in turn administers management services for hosts C5 and C6.

Because of the hierarchical arrangement of S1-S4 (and M1-M4), S1 is more secure than any of S2-S4, because S1 can transmit management messages to S2-S4, while none of S2-S4 can transmit management messages to S1. Thus S1 is secure, compared to S2-S4, thus being a secure location. Keep in mind that this is not a physical location, such as the National Cathedral, but rather is a network location. In Sudama, the more upstream a system is the more secure it is, and the more downstream a system is the less secure it is. Furthermore, note that in paragraph 15 of the instant specification, the Appellant discusses that the secure and non-secure locations form a hierarchy. This is similar to the teachings of Sudama, specifically in Col. 8 Paragraph 4. As such, the examiner believes that Sudama meets these limitations.

Regarding the Appellant's argument, regarding the rejection of claim 1 under 35 USC 102(b), that Sudama does not teach or suggest "determining a first list of nodes that may send or receive substantive communication in the secure network," the examiner disagrees. First, note that the examiner is reading the "management operations" of Sudama as the "substantive communications" of the claims (further note Page 28 Lines 11-13 of the brief appear to admit that management communications are substantive communication). Second, note that claim 1

does not recite "determining a first list of ***all*** nodes that may send or receive substantive communication in the secure network". Sudama, in Col. 8 Paragraphs 1-2, teaches that the systems are provided with lists "provided by the database 36 can be divided into two categories: trusted receivers of the management operations and trusted senders." This falls within the scope of the claim language, and as such the examiner believes that Sudama meets this claim limitation.

Therefore, the examiner believes that Sudama anticipated the limitations of claim 1, and therefore the rejection should be maintained.

Regarding the Appellant's argument, regarding the rejection of claim 35 under 35 USC 102(b), that Sudama does not teach or suggest that "a primary configuration node [is] configured or adapted to exclusively control a defined set of management functions throughout said secure network", the examiner disagrees. Sudama teaches in Col. 5 Paragraph 3, Col. 7 Lines 31-42, and Col. 8 Paragraph 4, that management server M1 of node S1, is the most upstream server, and that it is the only server that can process management services for host C1. This, in itself meets the limitation of the claim language. Furthermore, S1 is the only node which can send management operations to node S2, as is disclosed in Col. 8 Paragraph 4. As such, the examiner believes that Sudama meets this limitation.

Regarding the Appellant's argument, regarding the rejection of claim 35 under 35 USC 102(b), that Sudama does not teach or suggest "a memory for storing…device connection information specifying **[all]** nodes or ports that may send or receive **[any]** substantive communication in the secure network" the examiner notes that the claim language does not recite "all nodes or ports" or "any substantive communication", and in this case, as discussed above, the

examiner has read the "management operations" as the claimed "substantive communication". Furthermore, when looking at Fig. 2 of Sudama, the "nodes" are S1-S4, each containing "M1-M4". S1-S4, are the only nodes in the network disclosed by Sudama. As discussed above, the examiner believes that the lists of Sudama, discussed in Col. 8 paragraphs 1-2, meet this limitation.

Therefore, the examiner believes that Sudama anticipated the limitations of claim 35, and therefore the rejection should be maintained.

Regarding the Appellant's argument, regarding the rejection of claim 73 under 35 USC 102(b), that Sudama did not disclose "a plurality of devices including one or more switching and routing devices, ... all devices able to inter-communicate by forwarding communications through each other," the examiner disagrees. First, the examiner has interpreted the systems S1-S4 as reading on "the devices". Second, the claim language only recites that these devices are able to communicate in this manner. As such, in order for Sudama to not meet this limitation, there would need to be a specific teaching against this limitation in Sudama, which there is not. Moreover, the claim language neither recites that the all devices must be able to intercommunicate with all other devices, nor recites that each device is able to send and receive communications to and from each other device. Rather what the claim language requires is that all devices are able to inter-communicate (send or receive communications) by forwarding communications through each other. Note that in Sudama S1 comprises M1, S2 comprises M2, S3 comprises M3, and S4 comprises M4. In Col. 8 Paragraph 4 of Sudama, it is described that S1 and S2 are able to communicate directly, S1 and S3 communicate through S2, and S1 and S4

communicate through S2 and S3. Similarly, S2 and S3 can also communicate directly, and S2 and S4 can communicate through S3. Similar still, S3 and S4 can communicate directly. Furthermore, this is extremely common practice in the art of networking, as well as in the art of communications. For example, in order for me to send a letter to my mother through the postal mail network, there are many nodes that forward the communication, such as my local post office, and my mother's local post office, as well as other nodes. This is simply common sense.

Regarding the Appellant's argument, regarding the rejection of claim 73 under 35 USC 102(b), that Sudama did not disclose that "all of said devices carry a list of all devices allowed on the network", the examiner disagrees. Sudama disclosed in Col. 8 Paragraphs 1-2, that each management server (which is comprised by one of "devices" S1-S4) "stores the lists locally", the lists indicating trust relationships between all the management servers in the network. In Sudama, S1-S4 are the devices allowed in the network because they are all the devices in the network. Further still, Sudama Col. 8 Paragraph 3 disclosed that the lists include a namespace which designated management servers fore the specified hosts. Therefore, the "namespace" is a list of all devices on the network. Sudama does not state that any of these devices are not allowed to be on the network, but rather shows that all of these devices are allowed to be on the network by providing them with trust relationships to the other devices in the network. As such, the examiner believes that Sudama meets this limitation.

Therefore, the examiner believes that Sudama anticipated the limitations of claim 73, and therefore the rejection should be maintained.

Regarding the Appellant's argument, regarding the rejection of claims 2-12, and 36-46 under 35 USC 102(b), that Sudama did not disclose or suggest "node connection controls for

designating nodes to participate in the secure network", the examiner disagrees. Sudama, in Col. 4 Lines 28-31 and Col. 8 Paragraph 2, clearly disclosed that the lists maintained in the global database, which is stored in S1 as can be seen in Fig. 1, control the connections between the various nodes and their participation in the network. As such, the examiner believes that Sudama meets this claim limitation.

Regarding the Appellant's argument, regarding the rejection of claims 2-12, and 36-46 under 35 USC 102(b), that Sudama did not disclose or suggest "succession of primary configuration node", the examiner disagrees. Sudama, in Col. 8, clearly shows that the lists in the global database, which is maintained in S1, establish a hierarchy of control in the network, in a downstream manner. The examiner believes that this meets this limitation.

Therefore, the examiner believes that Sudama anticipated the limitations of claims 2-12, and 36-46, and therefore the rejection should be maintained.

Regarding the Appellant's argument, regarding the rejection of claim 13 under 35 USC 102(b), that Sudama did not disclose "allowing no management access to said secure network from nodes located in said less secure network" because there is no teaching of secure networks or less secure networks, which has been addressed above, or further because Sudama disclosed that each node S1-S4 contains a management server and thus has access to management, the examiner disagrees. The claim language states that a node in said less secure network (S4) has no management access ***to said secure network*** (S3 or S2 or S1) This is precisely what Sudama teaches, that downstream (less secure) locations cannot send management operations upstream. As such, the examiner believes that the claim limitation is met by Sudama.

Therefore, the examiner believes that Sudama anticipated the limitations of claims 13 and 47, and therefore the rejection should be maintained.

Regarding the Appellant's argument, regarding the rejection of claim 18-19, and 52-53 under 35 USC 102(b), that Sudama did not disclose that "the DCC list be distributed to every node in the secure network", the examiner disagrees. Sudama in Col. 8 Paragraph 1-2 disclosed that the lists are stored locally at every management server, and each "node" S1-S4 contains one of the management servers M1-M4. As such, the examiner believes that Sudama meets this limitation.

Therefore, the examiner believes that Sudama anticipated the limitations of claims 18-19, and 52-53, and therefore the rejection should be maintained.

Issue #3

Regarding the Appellant's argument, with respect to the rejection of claim 76 under 35 USC 103(a) in view of Sumada and FIPS, that Sudama and FIPS do not disclose or suggest "a memory…substantively communicate on the network", the examiner has addressed this argument above, and therefore has not addressed it again.

Regarding the Appellant's argument, with respect to the rejection of claim 76 under 35 USC 103(a) in view of Sumada and FIPS, that Sudama and FIPS did not disclose or suggest "at least one logical management access channel that may be disabled through network management control", the examiner disagrees. First, a logical channel is just a channel that is conceptually true to a design or an idea. In other words, it is just a channel in the broadest sense of the term, and a channel is just a path or link through which information passes between two devices.

Sudama teaches communication paths between then devices S1-S4, as can be seen in Fig. 2. Logically, the paths 44, 46, and 48 can thought of as having an upstream channel and a downstream channel, downstream being in the direction of S1 to S4. Sudama further teaches, as can be seen in Col. 8, that the lists of trusted paths dictate that no "trusted paths" exist for routing management operations upstream. The logical paths exist, as can be seen in Fig. 2, but the lists "disable" these paths by not allowing them to be used (i.e. no routing management operations upstream). Remember, it is important to note that the claimed "channel" is logical, and thus must only exist conceptually. As such, the examiner believes this limitation has been met by the combination of Sudama and FIPS.

Therefore, the examiner believes that Sudama and FIPS render obvious the limitations of claim 76, and therefore the rejection should be maintained.

Regarding the Appellant's argument, with respect to the rejection of claim 79 under 35 USC 103(a) in view of Sumada and FIPS, that Sudama and FIPS did not disclose or suggest "an [network configuration entity] NCE list...comprising an indication of each device in the network that may operate as said network configuration entity", the examiner disagrees. As discussed above, S1 has been equated to the NCE of the claim language because S1 has exclusive control over the management functions of S1 throughout the secure network. This is the only device which may operate as said NCE in the network of Fig. 2 of Sudama. Furthermore, Sudama teaches in Col. 8 that the list specifies that S1 is the only device which can perform management operations on S1, because no management operations may arrive at S1 from downstream and S1 is the most upstream device in the hierarchy. As such, the examiner believes that Sudama meets this limitation.

Regarding the Appellant's argument, with respect to the rejection of claim 79 under 35 USC 103(a) in view of Sumada and FIPS, that Sudama and FIPS did not teach or suggest "a…list comprising an indication of each device allowed to participate in said secure network" the examiner disagrees. As discussed above, Sudama teaches a list of all the trusted relations between the all the devices in the network, as can be seen in Col. 8 Paragraph 1, as well as a list (namespace) storing all the associated management server for each host in the network. The simple presence of the device being on either of these lists is an indication that it is allowed to participate in the secure network. As such, the examiner believes that the combination of Sudama and FIPS meets this limitation.

Therefore, the examiner believes that Sudama and FIPS render obvious the limitations of claim 79, and therefore the rejection should be maintained.

Regarding the Appellant's argument regarding the rejection of claims 72 and 74, that Sudama and Thapar did not teach or suggest "only allowing substantive communication between directly connected ports that have been mutually authenticated", the examiner disagrees. Sudama in Col. 5 Paragraph 3 states that management operations, which the examiner is reading as the substantive communications, may occur only if "2)the management servers participating in the forwarding operation are mutually authenticated". If the servers are mutually authenticated, then the physical ports where the paths 44, 46, and 48 connect to the servers are authenticated as well. As such, the examiner believes that the combination of Sudama and Thapar meet this claim limitation, and therefore the rejection should be maintained.

Therefore, the examiner believes that Sudama and FIPS render obvious the limitations of claims 72 and 74, and therefore the rejection should be maintained.

The examiner notes that the Appellant has not contested the rejection of claim 32 under 35 USC 103(a) in view of Sudama, FIPS, and Fischer, and as such the examiner believes that this rejection should be maintained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Matthew T Henning/
Examiner, Art Unit 2131
2/29/2008

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/GBJ/
Gilberto Barron, Jr.
Supervisory Patent Examiner
Art Unit 2132

/Christian LaForgia/
Christian LaForgia
Primary Patent Examiner
Art Unit 2139